INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

SECURE ROUTING MECHANISMS IN WIRELESS MOBILE NETWORKS

Dr.Hamela K
Associate Professor and Head,
Department of Computer Science,
Government First Grade College,
Kolar, Karnataka, India.

Abstract

Wireless Mobile Networks have become an essential component of modern communication systems due to their flexibility, mobility, and infrastructure-less operation. However, the open wireless medium makes these networks vulnerable to numerous security threats such as eavesdropping, packet dropping, routing manipulation, and denial-of-service attacks. Secure routing mechanisms are therefore critical for ensuring reliable data transmission and network integrity. This paper presents an overview of secure routing protocols and their significance in wireless mobile environments. Various security challenges, routing attacks, and defense mechanisms are discussed. Furthermore, secure routing protocols such as SAODV, ARAN, and SEAD are analyzed and compared. The study highlights the effectiveness of cryptographic techniques and trust-based approaches in enhancing routing security. Finally, future research directions for developing robust and scalable secure routing solutions are presented.

Keywords: Wireless Mobile Networks, Secure Routing, MANET, SAODV, ARAN, SEAD, Network Security, Routing Protocols.

I. Introduction

Wireless Mobile Networks enable communication among mobile devices without relying on fixed infrastructure. These networks are widely used in military operations, disaster recovery, healthcare monitoring, and intelligent transportation systems. Due to node mobility and dynamic topology, routing becomes a challenging task. Traditional routing protocols mainly focus on performance metrics such as delay and throughput but often neglect security requirements. The wireless medium allows attackers to intercept, modify, or disrupt communication. Therefore, secure routing mechanisms are required to protect routing information and data transmission. Secure routing protocols employ authentication, encryption, and trust management techniques to prevent malicious activities. This paper examines various routing threats and explores

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

secure routing solutions for wireless mobile networks.

II. Wireless Mobile Network Architecture

Wireless Mobile Networks are composed of autonomous mobile nodes that communicate over wireless channels without requiring fixed infrastructure. Each node functions as both a communication endpoint and a router, forwarding packets for other nodes. The network topology changes frequently due to node mobility, making routing decisions dynamic and challenging. These networks are particularly useful in environments where deploying fixed infrastructure is impractical, such as disaster recovery operations, military battlefields, emergency response systems, and remote sensing applications. Communication in wireless mobile networks generally occurs through multi-hop routing, where intermediate nodes relay packets between source and destination nodes.

Because nodes may join or leave the network at any time, routing protocols must continuously update routing information. Furthermore, limited battery power, restricted bandwidth, and security vulnerabilities make efficient and secure routing mechanisms essential for maintaining reliable communication.

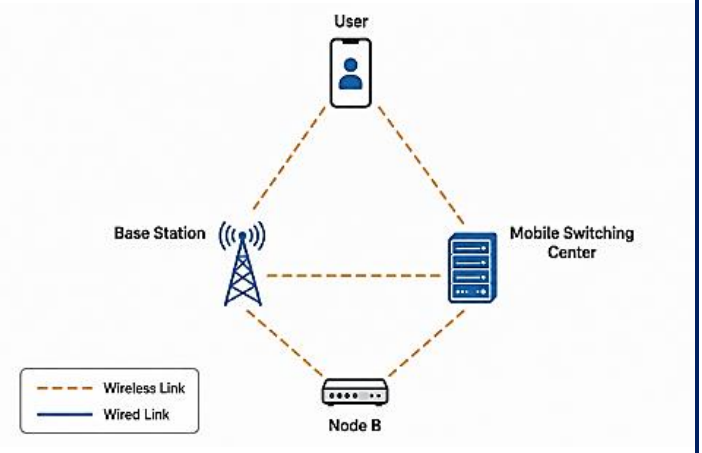

Figure 1: Wireless Mobile Network Architecture

Characteristics of Wireless Mobile Networks

- **Dynamic Network Topology:** Nodes move freely, causing frequent changes in network structure.
- **Limited Bandwidth:** Wireless channels offer lower bandwidth compared to wired networks.
- **Decentralized Operation:** No centralized controller exists; all nodes cooperate in routing.
- **Energy Constraints:** Mobile devices operate on batteries and require energy-efficient protocols.
- **Multi-hop Communication:** Data packets travel through multiple intermediate nodes.
- **Self-Configuring Capability:** Nodes automatically organize and manage network operations

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

III. Security Requirements in Wireless Mobile Networks

Table 1: Secure routing protocols must satisfy the following security objectives

Security Requirement	Description
Authentication	Verifies the identity of communicating nodes
Confidentiality	Prevents unauthorized access to data
Integrity	Ensures data is not altered during transmission
Availability	Guarantees network services remain accessible
Non-Repudiation	Prevents denial of participation in communication
Access Control	Restricts unauthorized network access

IV. Routing Attacks in Wireless Mobile Networks

Wireless mobile networks are vulnerable to various routing attacks.

A. Black Hole Attack

A malicious node falsely advertises itself as having the shortest route to the destination and drops all received packets.

Source ----> Malicious Node ----X----> Destination

(Packets Dropped)

Figure 2. Black Hole Attack Model

B. Wormhole Attack

Two colluding attackers create a tunnel to manipulate routing information.

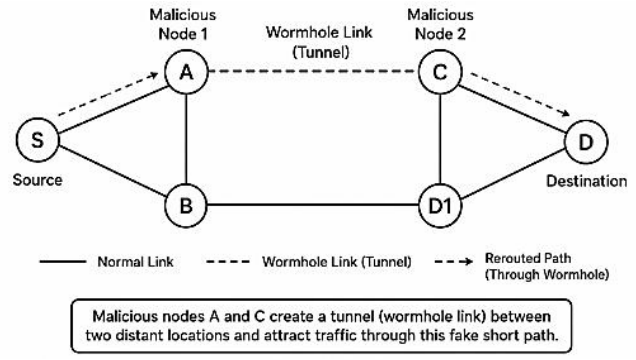

Figure 3. Wormhole Attack

C. Sybil Attack

A single malicious node assumes multiple fake identities to influence routing decisions.

D. Denial of Service (DoS) Attack

Attackers flood the network with excessive traffic, reducing network availability.

V. Secure Routing Mechanisms

Several approaches have been proposed to improve routing security.

A. Cryptographic-Based Routing

Cryptographic techniques protect routing messages through encryption and digital signatures.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

Advantages

- Strong authentication
- Message integrity
- Resistance against spoofing attacks

Limitations

- Computational overhead
- Increased energy consumption

B. Trust-Based Routing

Trust management systems evaluate node behavior and assign trust values.

Working Principle

Node Monitoring
↓
Trust Calculation
↓
Trust Update
↓
Route Selection

Benefits

- Detects malicious nodes
- Improves routing reliability
- Supports dynamic environments

C. Intrusion Detection Systems (IDS)

IDS continuously monitors network activities to identify suspicious behavior.

Table 2: Network Intrusion Detection System Components and Functions

Component	Function
Data Collection	Captures network activities
Analysis Engine	Detects anomalies
Alert System	Reports attacks
Response Module	Takes corrective actions

VI. Secure Routing Protocols

A. Secure AODV (SAODV)

SAODV extends the AODV routing protocol by incorporating digital signatures and hash chains.

Features

- Route authentication
- Protection against route manipulation
- Secure route discovery

B. Authenticated Routing for Ad Hoc Networks (ARAN)

ARAN utilizes certificates issued by trusted authorities.

Features

- End-to-end authentication
- Non-repudiation
- Protection against spoofing

C. Secure Efficient Ad Hoc Distance Vector (SEAD)

SEAD employs one-way hash functions to secure routing updates.

Features

- Low computational complexity
- Protection against routing table tampering
- Efficient route maintenance

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

Table 3: Comparative Analysis of Secure Routing Protocols

Protocol	Authentication	Encryption	Attack Resistance	Overhead
SAODV	High	Yes	High	Medium
ARAN	Very High	Yes	Very High	High
SEAD	Medium	No	Medium	Low
Trust-Based Routing	Medium	Optional	High	Medium
IDS-Based Routing	Medium	No	High	Medium

VII. Performance Evaluation Metrics

The effectiveness of secure routing protocols is measured using the following metrics:

Table 4: Evaluation Metrics and Their Descriptions

Metric	Description
Packet Delivery Ratio	Successfully delivered packets
Throughput	Data transmitted per second
End-to-End Delay	Average transmission delay
Routing Overhead	Control packets generated
Detection Rate	Percentage of attacks detected
Energy Consumption	Battery power utilized

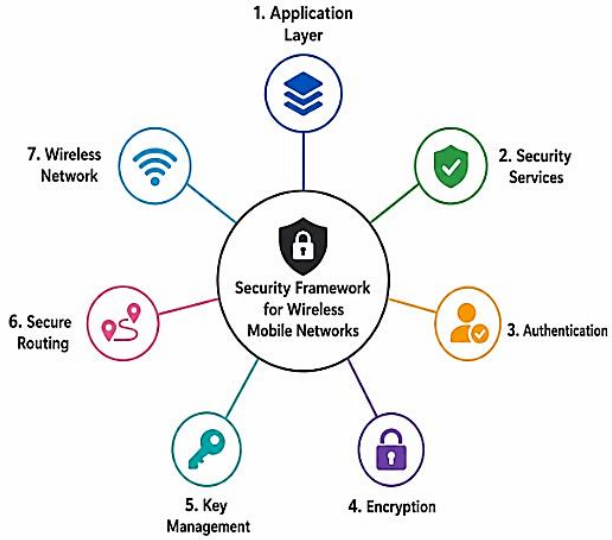

Figure 4: Security Framework for Wireless Mobile Networks

IX. Future Research Directions

- AI-based secure routing protocols.
- Blockchain-enabled trust management.
- Lightweight cryptographic algorithms for IoT devices.
- Energy-efficient secure routing mechanisms.
- Machine learning-based intrusion detection systems.
- Quantum-resistant security techniques for next-generation wireless networks.

X. Conclusion

Wireless Mobile Networks offer flexible and cost-effective communication solutions but are highly susceptible to security threats due to their decentralized and dynamic nature. Secure routing mechanisms play a vital role in protecting routing information and ensuring reliable data transmission. This

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 29 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-718 PAGE NO: 025-030

paper reviewed major routing attacks, security requirements, and secure routing protocols including SAODV, ARAN, and SEAD. Comparative analysis indicates that no single protocol provides complete security while maintaining low overhead. Therefore, hybrid approaches combining cryptography, trust management, and intrusion detection techniques are recommended. Future developments involving artificial intelligence and blockchain technologies are expected to further strengthen routing security in wireless mobile networks.

References

1. C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proceedings of IEEE WMCSA, pp. 90–100, 1999.
2. Y. Hu, A. Perrig, and D. Johnson, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, vol. 1, no. 1, pp. 175–192, 2003.
3. K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proceedings of IEEE ICNP, pp. 78–87, 2002.
4. B. Dahill, B. Levine, E. Royer, and C. Shields, "ARAN: A Secure Routing Protocol for Ad Hoc Networks," University of Massachusetts Technical Report, 2002.
5. L. Zhou and Z. Haas, "Securing Ad Hoc Networks," IEEE Network, vol. 13, no. 6, pp. 24–30, Nov. 1999.
6. P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.
7. A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, 2004.
8. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38–47, 2004.